(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 14 682 A 1**

(51) Int. Cl.[6]:
G 07 C 9/00
G 06 K 9/00

(21) Aktenzeichen: P 44 14 682.5
(22) Anmeldetag: 27. 4. 94
(43) Offenlegungstag: 2. 11. 95

DE 44 14 682 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Heywang, Walter, Prof. Dr., 85630 Grasbrunn, DE

(54) Sicherheitssystem mit Unterschriftsverifikation für kontrollierten und beweisfähig dokumentierten Zugang/Zugriff

(57) Die Erfindung betrifft ein in sich geschlossenes Sicherheitssystem für kontrollierten und beweisfähig dokumentierbaren Zugang/Zugriff von Personen zu einem sicherheitsrelevanten Bereich. Die Abgeschlossenheit des Identifikationssystems ermöglicht einen auf das jeweilige Problem zugeschnittenen und damit kostengünstigen Aufbau und hohe Verifikationssicherheit auch bei minimalem Bit-Bedarf für das Referenzmuster. Eine Erstellung des Referenzmusters im systemeigenen Zentralcomputer steigert die zu erzielende Sicherheit.

DE 44 14 682 A 1

Die folgenden Angaben sind

Beschreibung

Die vorliegende Erfindung bezieht sich auf ein Sicherheitssystem für kontrollierten und beweisfähig dokumentierten Zugang/Zugriff von Personen zu einem sicherheitsrelevanten Bereich.

Aus Druckschriften zahlreicher Untersuchungen und Vorschläge ist bekannt, die Echtheit einer aktuell geleisteten Unterschrift mit Hilfe einer vergleichenden Rechneranalyse ihrer dynamischen Charakteristika (Features; Parameter) zu verifizieren.

Bei einem dynamischen Verfahren zur Unterschriftsverifikation werden bestimmte Charakteristika einer aktuell zu leistenden Unterschrift auf ihr Vorhandensein (bzw. Fehlen) im Unterschriftszug überprüft, und zwar dies im Vergleich zu einem vorliegenden Referenzmuster und dessen dynamischen Daten. Ganz allgemein werden dazu generelle individuelltypische, d. h. individuumsgebundene Charakteristika herangezogen. Man kann dabei lokale und globale Charakteristika bzw. Parameter unterscheiden. Erstere sind beispielsweise die lokale Geschwindigkeit, Beschleunigung, Krümmung und dgl. an bestimmten Stellen innerhalb des Unterschriftszuges. Globale Parameter sind u. a. die maximale oder minimale Anzahl von Spitzen, Signallängen, Anzahl von Segmenten und dgl.

Für die Brauchbarkeit eines Systems zur Verifikation einer Unterschrift kommt es wesentlich darauf an, die Echtheit möglichst zuverlässig zu verifizieren, dabei aber Zurückweisungen von tatsächlich echten Unterschriften, d. h. falsche Zurückweisungen möglichst zu minimieren. Das Problem ist nämlich, daß Personen abhängig von verschiedensten Einflüssen und Gegebenheiten ihre Unterschrift nicht immer mit wenigstens nahezu identischem dynamischem Schriftzug leisten, es sich aber dennoch immer um echte Unterschriften ein und derselben Person handelt. Es ist dementsprechend üblich, aus einer Vielzahl zuvor unter verschiedenen Umständen geleisteter Unterschriftsproben ein Referenzmuster mit einem jeweiligen Toleranzbreitebereich für die einzelnen Charakteristika zu erstellen. Bei innerhalb dieser Bereiche liegenden Variationen einer geleisteten Unterschrift wird diese als echt anerkannt.

Der Stand der Technik enthält zahlreiche Beschreibungen, in welcher Weise ein solches Referenzmuster mit Toleranzbereich für eine jeweilige Person zu erstellen ist. Daher bedarf es hier keiner weiteren Beschreibung solcher einschlägig bekannter technischer Maßnahmen.

Trotz der intensiv betriebenen Arbeiten auf diesem Gebiet der Unterschriftsverifikation fehlt es aber an praktisch einsatzfähigen Systemen, die zu dem jeweiligen Anwendungsfall technisch und auch preislich akzeptabel angepaßt sind.

Aufgabe der Erfindung ist es, ein Anwendungsgebiet und ein auf dieses Anwendungsgebiet gezielt angepaßtes Sicherheitssystem anzugeben, bei dem der Umfang der erfindungsgemäß anzuwendenden Verifikationsmaßnahmen auf den Anwendungsfall zugeschnitten bemessen ist. Mit der Erfindung soll ein jeweils vorgegeben bestimmtes Bedürfnis mit einem Minimum an notwendigen technischen Maßnahmen befriedigt werden, dennoch aber genügende Sicherheit der Verifikation gewährleistet sein. Insbesondere soll mit der Erfindung sichergestellt sein, daß nicht solche Dritte Zugang/Zugriff erlangen können, die sich als Unbefugte in den Besitz des "Schlüssels" gebracht haben, wobei auch der Fall einer Besitznahme eingeschlossen ist, der mit Zwang oder Bedrohung erreicht worden ist.

Die der Erfindung zugrunde liegende Aufgabe wird mit den Merkmalen des Anspruches 1 gelöst. Weitere Ausgestaltungen geben Unteransprüche an.

Die Erfindung ist ein Sicherheitssystem, das nicht nur für den kontrollierten, sondern auch für den beweisfähig dokumentierten Zugang/Zugriff von Personen zu einem sicherheitsrelevanten Bereich ausgestaltet ist. Dieses Sicherheitssystem ist erfindungsgemäß darauf ausgelegt, daß es sich bei den zu berücksichtigenden Personen um einen ausgewählten/vorgegebenen Kreis mit relativ geringer Personenanzahl handelt. Spezielle Anwendungsgebiete der Erfindung sind z. B. der Safe-Raum einer Bank, für dessen Betreten nur die Anzahl Personen in Betracht kommt, denen in dieser Bank hierfür die Bevollmächtigung erteilt ist. Im Falle von Kundensafes ist z. B. der Personenkreis durch die Anzahl der vorhandenen Kundenfächer von vorneherein überschaubar begrenzt. Ein anderer Anwendungsfall ist z. B. der Zutritt zu sicherheitsrelevanten Räumen, z. B. im Industrie-, Militär- und/oder Verwaltungsbereich, von deren Betreten alle Unbefugten mit Sicherheit ausgeschlossen sein sollen.

Für die Erfindung ist als voranstehende Bedingungen insgesamt optimal erfüllend die dynamisch aktuell zu leistende Unterschrift als geeignetes Mittel der Verifikation erkannt worden. Eine Unterschrift kann man im Gegensatz zu einer PIN-Nummer weder vergessen noch gewollt oder gar unter Zwang weitergeben. Unter physischer Gewalt wird eine Person im Regelfall nur eine solche Unterschrift leisten (können), die dann wegen zu starker Abweichungen vom Referenzmuster vom erfindungsgemäßen System nicht akzeptiert werden wird, obwohl sie an sich echt ist.

Die Begrenzung auf einen relativ kleinen Personenkreis von z. B. nicht mehr als 10 oder z. B. von nicht mehr als 100 oder 500 Personen (letzteres z. B. im Falle von Kundensafes) kann das System leicht auf eine solche Anzahl angepaßt bemessen werden. Vorzugsweise ist diese besonders angepaßte Bemessung auf die Wahl der Anzahl der zu überprüfenden Charakteristika der jeweiligen individuellen Unterschrift ausgerichtet. Es können sogar erfindungsgemäß aus einem jeweiligen Unterschriftszug besondere Charakteristika als kennzeichnend ausgewählt werden, die generell in Unterschriftszügen nicht auftreten oder zur Verifikation generell ungeeignet sind. Wesentlich ist nur, daß die zur Verifikation herangezogenen Charakteristika auf besonderen individuell eingeübten und eingewöhnten dynamischen Muskelbewegungen im Handgelenk der betreffenden Person beruhen, die von einem Dritten sowohl in Form als auch mit der Geschwindigkeit des Referenzmusters nicht nachgeahmt werden können.

Bei der Erfindung ist vorgesehen, das Referenzmuster zur aktuell auszuführenden Unterschrift der Person in einer Smart-Card, sonst aber nirgendwo anders zu speichern. Letzteres dient dazu, Möglichkeiten einer Manipulierbarkeit auszuschließen und z. B. auch die Dokumentation beweisfähig zu machen.

In der Smart-Card der jeweiligen Person ist in der Form von gespeicherten Bits ein Referenzmuster vorzugsweise ausgewählter Charakteristika der Form und der Dynamik der Unterschrift gespeichert. Dieses Referenzmuster umfaßt aber auch die notwendigen Toleranzbreiten, denn es ist bekannt, daß ein und dieselbe Person insbesondere unter verschiedenen Bedingungen nicht einmal nahezu identische Unterschriftszüge leistet. Solche unterschiedlichen Bedingungen können z. B. un-

terschiedliche Höhe des Tableaus auf dem die Unterschrift zu leisten ist, die Umgebungstemperatur, vorangegangene Anstrengung der Hand, z. B. durch Tragen, und dergleichen vieles mehr sein.

Besonders invariante und daher bevorzugte Charakteristika einer Unterschrift sind Schreibansätze des Anfangs und ggfs. innerhalb des Unterschriftszuges, nach oben weisende Spitzen oder Ecken, nach unten weisende Spitzen oder Ecken, rechte Kurven und linke Kurven des Schriftzuges und insbesondere auch die zeitlichen linearen Abstände solcher aufeinander folgender Ekken/Spitzen, rechter/linker Kurven und der ggfs. vorhandenen Ansätze voneinander. Solche Größen werden dann für das Referenzmuster zeitnormiert. Der Aufwand hierfür und auch die zu berücksichtigenden Toleranzbreiten können insbesondere dadurch noch verringert werden, daß in dem erfindungsgemäßen System der Platz bzw. die Fläche, innerhalb der die aktuell zu leistende und für die Freigabe des Zugangs/Zugriffs zu verifizierende Unterschrift hinzuschreiben ist, flächenmäßig begrenzt vorgegeben bemessen ist. Die zu leistende Unterschrift hat dann im wesentlichen immer dieselbe Größe, wodurch dann die Toleranzbreite enger bemessen werden kann, ohne daß eine höhere Rate fehlerhafter Zurückweisungen zu erwarten ist.

Für die Erstellung des in der Smart-Card zu speichernden Referenzmusters der jeweiligen Unterschrift bzw. ihrer Form- und Dynamikcharakteristika können die bekannten Methoden und Geräte benutzt werden. Eine Besonderheit der Erfindung liegt darin, daß man den Randbedingungen entsprechend relativ geringe Bit-Anzahl, d. h. relativ geringes Speichervolumen in der Smart-Card benötigt.

Ein erfindungsgemäßes Sicherheitssystem kann vorteilhafterweise als ein (eine) für sich geschlossenes System (Anlage) mit einem eigenen (entsprechend kleinen) Zentralcomputer realisiert werden. Ein besonderer technischer und sicherheitsrelevanter Vorzug ist dabei der, daß die Smart-Card und das in ihr gespeicherte Referenzmuster in diesem bzw. mit Hilfe dieses Zentralcomputers erstellt werden kann. Es wird von diesem Zentralcomputer bei der Erstellung des Referenzmusters der jeweiligen Unterschrift nicht nur der schon oben angesprochene Toleranzbereich für die einzelnen und insbesondere für die dynamischen Charakteristika berücksichtigt, sondern in diesem individuellen Zentralcomputer kann auch eine entsprechend individuelle Verschlüsselung der gespeicherten Informationen bzw. des erstellten Referenzmusters vorgenommen werden. Da dies mit dem dem Zentralcomputer eigenen Schlüssel erfolgt, kann kein (unbefugter) Dritter die Entschlüsselung vornehmen. Andererseits kann dieser für den einzelnen Sicherungsfall (Safe und dgl.) speziell angepaßte Zentralcomputer natürlich problemlos sein eigenes von ihm selbst verschlüsseltes Referenzmuster und die aktuell gelieferte Unterschrift miteinander verifizierend vergleichend verarbeiten.

Als Weiterbildung der Erfindung ist vorgesehen, die Funktionsfähigkeit der Smart-Card in dem System dann zu zerstören, wenn nach einer ersten, zweiten oder dritten Zurückweisung der geleisteten Unterschrift durch das System dann noch weitere Unterschriftenversuche angestellt werden. Bei solchen Fällen handelt es sich nämlich, Derartiges ist auch aus dem Stand der Technik bekannt, im Regelfall um den Versuch, mit einer Fälschung Zugang/Zugriff zu erlangen.

Da das erfindungsgemäße System auf den jeweils einzelnen Anwendungsfall zugeschnitten bemessen und ausgestaltet ist, ist es bzw. kann es vollständig kompatibel mit bereits vorhandenen Systemen gemacht werden. Ein erfindungsgemäßes System kann also ohne weiteres auch als lediglich Erweiterung eines schon vorhandenen Sicherheitssystems zur Erhöhung von dessen Sicherheitsgrad benutzt werden.

Die oben erwähnte beweisfähige Dokumentation des Vorganges ist durch die geleistete Unterschrift, und zwar diese insbesondere zusammen mit Datum und ggfs. Uhrzeit, gewährleistet. Die Unterschrift wird dazu z. B. mit einem Schreibstift auf einem Blatt Papier geleistet, das auf dem die geleistete Unterschrift ansonsten elektronisch abtastenden Graphiktableau aufgelegt ist. Dieses Blatt kann dann eine geeignete Zeitlang als gerichtlich anerkanntes Dokument aufbewahrt werden.

Die Figur zeigt ein Prinzipbild eines erfindungsgemäßen Systems. Mit **1** ist ein z. B. Graphiktableau bezeichnet, auf dessen Oberfläche die zu leistende Unterschrift zu schreiben ist und das die Daten der elektrischen Abtastung liefert. Mit **2** ist eine Einrichtung zur Erstellung eines Bitmusters der Unterschrift bezeichnet. Das Bitmuster wird dort nach den Vorgaben erstellt, nach denen auch das dem Referenzmuster zugrundeliegende Bitmuster (dort aus mehreren Unterschriftsproben gemittelt) erstellt worden ist. Dieses Bitmuster wird als Eingabemuster **3** an eine Einrichtung **4** gegeben, die in an sich bekannter Weise einen Mustervergleich ausführt, nämlich einen Vergleich mit dem Referenzmuster **5** des Kartenlesers **6**. Dieses Referenzmuster **5** ist in der Smart-Card **7** gespeichert. Im Mustervergleich **4** erfolgt der Vergleich der vorgegebenen Form- und Dynamik-Charakteristika.

Eine wie in der Figur angegebene Elektronikeinrichtung wird z. B. am Eingang des zu schützenden Sicherheitsbereiches angebracht. Die Zugang begehrende Person muß in diese Einrichtung ihre Smart-Card einführen und auf dem Graphiktableau **1** die Unterschrift leisten. Anerkennt der Mustervergleich hier die Unterschrift als innerhalb der Toleranzbreite des Referenzmusters **5** liegend, liefert der Mustervergleich ein z. B. für eine Relaissteuerung geeignetes Signal **8**, mit dem der übliche Verschluß des Zugangs (Tür, Gitter oder dgl.) für das Eintreten freigegeben wird.

Patentansprüche

1. Sicherheitssystem für kontrollierten und beweisfähig dokumentierten Zugang/Zugriff von Personen zu einem sicherheitsrelevanten Bereich,
wobei es sich bei diesen Personen um einen ausgewählten/vorgegebenen Kreis derselben handelt, und deren bei Zugang/Zugriff aktuell zu leistende Unterschrift als jeweiliges individuelles Verifikationsmittel in der Weise ausgewertet wird,
daß in einer Einrichtung dieses Systems diese aktuell geleistete Unterschrift auf das Vorhandensein vorgegebener ausgewählter individueller dynamischer Schriftcharakteristika derselben im Vergleich mit einem vorhandenen Referenzmuster auf Übereinstimmung überprüfbar ist, wobei das Referenzmuster dieselben Charakteristika umfaßt und dieses Referenzmuster als Bit-Muster allein in einer in diese Einrichtung einzuführenden Smart-Card gespeichert enthalten ist, und
wobei die Anzahl der vorgegeben ausgewählten individuellen Charakteristika auf die Anzahl Personen des vorgegebenen Personenkreises abgestimmt derart bemessen ist, daß das notwendige

Maß an Sicherheit der Verifikation bereits erreicht ist.

2. Sicherheitssystem nach Anspruch 1, bei dem das Referenzmuster ausschließlich in der Smart-Card gespeichert ist.

3. Sicherheitssystem nach Anspruch 1 oder 2, bei dem der Zentralcomputer des Systems so ausgestaltet ist, daß mit diesem das Referenzmuster der Unterschrift erstellt ist.

4. Sicherheitssystem nach Anspruch 3, bei dem der Zentralcomputer eine eigene Verschlüsselungseinrichtung für die Information des Referenzmusters enthält.

5. Sicherheitssystem nach einem der Ansprüche 1 bis 4, bei dem für das Referenzmuster der Unterschrift einer jeweils einzelnen Person auch ein solches Charakteristikum ausgewählt ist, das nur der Unterschrift dieser Person zu eigen ist.

6. Anwendung eines Sicherheitssystems nach einem der Ansprüche 1 bis 5 für die Kontrolle des Zugangs/Zugriffs zu einem Banksafe.

7. Anwendung eines Sicherheitssystems nach einem der Ansprüche 1 bis 5 für die Kontrolle des Zugangs/Zugriffs zu einem sicherheitsrelevanten Bereich.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 44 14 682 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 2. November 1995